March 2018

SecurityAwarenessNews

the security awareness newsletter for security aware people

How IT Does It

Understanding Insider Threats

Understanding the Attackers

The Threat Connection

The Threat Connection

Have you ever considered a printer as a threat to your security? Probably not.

Imagine a scenario where everything you print is stored on a local hard drive and also accessed by a cybercriminal who has compromised your network. How much sensitive information would get stolen? Seems unreal, right? Unfortunately, you can't make this stuff up. Years ago, printer threats and vulnerabilities were proven in the lab. Last year, another group of researchers revealed even more vulnerabilities in network connected printers that leave backdoors open to attackers. One of the big problems? Leaving the printer user-ID and passwords set to factory defaults.

For all the convenience we like in our technologies, one ugly side effect impacts everyone: crime. From our mobile phones to our inboxes, the massive attack surface continues to grow. And the threats we face aren't always that obvious, such as with 'innocent' looking printers.

That's why we prioritize threat detection: not only to identify existing threats, but to identify the risks we take when using any technology. Anything connected to our networks can pose a threat. Individuals who have access to data and our networks can take risky actions, intentionally or not. And of course, many external malicious actors factor in as threats. Threat detection is modelled after the 3 Domains Triad, requiring technical, physical, and human efforts.

In the Cyber Domain, you identify scams and phishing emails. We do our best to thwart other cyber threats with controls like firewalls and network analytics before they can reach a human. You identify threats in the Physical Domain, like random USB drives or suspicious packages found in a parking lot. In the People Domain, you report anyone who doesn't belong or is acting strangely. And most importantly, you, along with all of your co-workers' keen awareness and threat detection efforts, always follow policy.

If you ever question your role within our organization in terms of identifying and reporting threats, or want to learn more about our threat detection policies, please ask!

APT's

Short for advanced persistent threats, APTs present the most sophisticated challenge, often launched by nation-states and organized groups of cybercriminals. Most APTs begin with phishing or social engineering attacks.

Ransomware

This malicious software locks up your devices and computers until you pay a specified ransom to the attacker. Experts advise against paying the ransom since there's no guarantee you'll regain access to your files. Restoring files from a good backup is the fastest solution.

Spear Phishing

Phishing ranks as the top threat we face both personally and professionally. Spear phishing targets specific people, industries, and organizations by utilizing stolen intel such as compromised email addresses.

Malicious Media

Just a few months ago, the Criminal Investigation Bureau in Taiwan inadvertently distributed over 50 USB drives that contained malware, highlighting the untrustworthiness of random media.

Humans

Most data breaches over the last few years were made possible by human mistakes or negligence, proving that cybersecurity is much more than defending against sophisticated criminal hackers. Stay alert, use common sense, and always follow policy!

How IT Does It

Ever wonder what goes on behind the scenes as organizations around the world battle cybercrime? Let's take a quick look at a few technologies that the good guys and gals in IT departments have at their disposal.

Machine Learning

Machine learning, one of the most exciting advancements in cybersecurity, uses algorithms to dynamically assess threats. **This means the software learns behaviors** of millions and millions of data points, and logs changes in behaviors to identify potential threats. For example, if a computer suddenly started consuming a large amount of network traffic, the algorithms would note this change and alert the appropriate parties as necessary. Machine learning, AI, and a host of similar buzzword products promise great things, but these are early-adopter technologies that still pose many unexplored risks.

Database Activity Monitoring

As data exposure grows, it becomes nearly impossible for IT personnel to track every single change or potential vulnerability. The solution to this problem is database activity monitoring, or DAM, which **audits changes and activity across networks**. DAM tracks both internal and external threats, as it monitors activity of privileged users, applications, and cyberattacks.

Intrusion Detection Systems

There are two basic types of intrusion detection systems (IDS): network and host. Network intrusion detection systems **monitor traffic to and from devices on a network**. Host intrusion detection systems run on individual devices and **monitor inbound and outbound traffic**. A simple example of an IDS that you're familiar with is antivirus software.

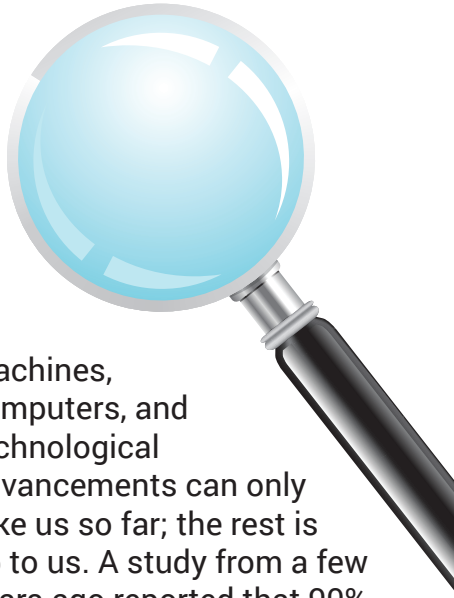
Penetration Testing

How can we know where our vulnerabilities exist without thoroughly assessing our risks? That's the concept behind penetration testing. It's a process in which **a third party is hired to break into networks and report vulnerabilities.** Automated online penetration services offer tailoring to organizations for specific security needs. Organization-sponsored phishing campaigns (where we intentionally phish all employees) is an example of penetration testing.

Threat Hunting

Even though we have access to several advanced technical solutions designed to eliminate threats, we will never achieve a 100% secure environment. For this reason, organizations utilize threat hunting, which is exactly what it sounds like: **a manual or machine-assisted process of searching networks to detect advanced threats that have circumvented other levels of protection**. Ongoing advancements in cybercrime technology require organizations to routinely hunt threats. Threat hunting, akin to Bug Bounties, aims to find errors in software.

Advanced Threat Detection & You



Machines, computers, and technological advancements can only take us so far; the rest is up to us. A study from a few years ago reported that 90% of phishing emails never make it through spam filters. That, of course, means 10% of phishing attempts do, in fact, reach our inboxes, which seems like a small number until you realize that 10% of all phishing attempts equals 16 million emails. These staggering numbers lead us to believe that **our most advanced form of threat detection comes down to you**, the human firewall. Security is not a just a state-of-the-art technological process; it's a mindset and part of our organization's culture. What's your role in all of this?

Stay informed.
Think before you click.
Report all security incidents immediately.
And always follow policy.

Understanding Insider Threats

As an important member of our organization, your user-privileges give you access to our data and networks. But that same access makes you a threat to our data and networks.

The Accidental Insider

April, one of the network gurus, is updating user privileges and **inadvertently deletes an entire portion of the database**.

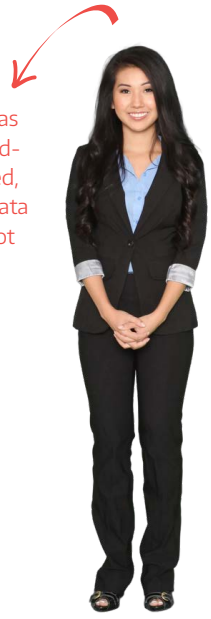
Being an insider threat isn't always about negligence or ill-intent. Accidents, such as deleting important files or sending data to the wrong party, have an impact just as big.

The Negligent Insiders

Way behind on work after vacation, Mateo **decides to take sensitive company files on a USB drive** so he can catch up, even though he knows this violates policy.

This is an example of an employee breaking company policy. Those that intentionally put sensitive data in harm's way, even with good intentions, fall under the category of negligent insiders.

While on a business trip, Chelsea's **organization-issued laptop was stolen** when she wasn't paying attention at a street café.



Lack of physical awareness could make you a negligent insider! Security depends not only on digital protections like encryption and passwords, but on the physical state of the devices on which data lives.

The Malicious Insider

Max recently learned that he will be included in a wave of layoffs. **So, he makes copies of marketing strategy documents hoping to sell them to a competitor**.

A malicious insider threat provides a tricky challenge for organizations to get in front of. Unfortunately, mitigation isn't always possible, as in this example.

It may sound harsh, but anyone with inside access to our organization could become an insider threat. That's the nature of doing business in an environment that handles sensitive data. But by working together, we can reduce our risk! Here's what you can do to help:

Report all incidents.
Phishing emails. Unusual amounts of spam. Someone not wearing a badge. Secured doors left unlocked... all of it needs to be reported ASAP.

Click with care.
Or don't click at all. Know how to spot phishing emails or scams, which often contain malicious links and attachments.

Verify the source.
Sending sensitive info to someone? Make sure you address the email to the right person and that they are authorized to receive sensitive info.

Stay alert.
In order to report security incidents, you need to be aware of them first! Don't snooze on security. Keep your eyes open and use common sense.

Always follow policy.
Our organizational efforts to identify and mitigate threats will fail if you ignore the policies we've carefully designed. Following policy helps secure our organization.

UNDERSTANDING THE ATTACKERS

In a lot of cases, knowing the ***why*** proves just as valuable as knowing the ***how***. If you've ever watched or read crime dramas, then you understand the word "intent." Investigators usually spend a lot of early efforts on solving the intent of a crime. Why was the crime committed? What was the motive? Understanding the **why** opens the door to serving justice. When it comes to security, understanding criminal motives has a direct impact on what we protect and how we do it.

WHAT — Personally Identifiable Information

Known simply as PII, this data includes a long list of items that can specifically identify an individual, such as full names, home addresses, and national ID numbers (to name a few).

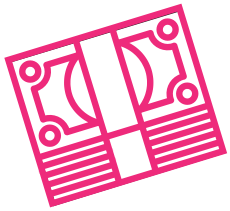
WHY — ID Theft

Identity theft ranks near the top as one of the most common crimes worldwide. By stealing your ID, criminals can act in your name. They can leverage your credit score to open accounts, file fraudulent insurance claims, and basically do anything you can do with your information. Here are five ways to prevent this from happening: https://www.thesecurityawarenesscompany.com/2017/03/23/five-ways-prevent-identity-theft/

WHAT — Usernames and Passwords (Online Accounts)

Although login credentials fall under the PII umbrella, criminals want them for more than just ID theft. Your usernames and passwords unlock a world of opportunity.

WHY — Cash



Gaining unauthorized access to any account, like email or social media, may lead to gaining access to other, more important accounts such as banks and credit cards. In this situation, the attacker can steal directly from you, or even sell your information on the dark web.

WHAT — Usernames and Passwords (Internet of Things)

Everything we connect to the internet, from routers to dishwashers (Internet of Things), opens another door for criminals.

WHY — DDoS Attacks

Distributed denial-of-service (DDos) attacks take down major servers by flooding them with more "hits" than they can handle. The results crash the servers and destroy all internet traffic that goes through them for extended periods of time. The easiest way to launch a DDoS attack stems from hacking smart devices, turning them into a botnet—tens of thousands of compromised devices used as an army. Botnets are often made possible by lax security settings of smart devices, especially default usernames and passwords.

WHAT — Email Addresses

Also considered PII, email addresses by themselves may not seem all that threatening. But when criminals gather thousands of them, the results can lead to disaster.

WHY — Phishing Campaigns

Phishing is the most successful social engineering tactic to date. Phishers launch campaigns aimed at specific companies or people (known as spear phishing) in hopes of spreading dangerous Trojans such as ransomware or other forms of malicious software.